HOME DEVICE AUTHENTICATION SYSTEM AND METHOD

[01] This application claims benefit under 35 U.S.C. § 119 from Korean Patent Application No. 2003-22981, filed on April 11, 2003, the entire content of which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

[02] Apparatuses and methods consistent with the present invention relate to a home network system, and more particularly, to a home device authentication system and a method performing a home device authentication process for home network system security.

2. Description of the Related Art

[03] High-speed access to the Internet, which is possible with x-Digital Subscriber Lines (xDSLs) or cable modems spread over many homes, together with development of the Internet in recent years, have explosively increased access to the Internet from personal home computers.

[04] Users want to do more than merely access the Internet, and many users expect to control and communicate with devices at home through personal computers. On the other hand, home network systems have been developed that enable the users to communicate with home devices and receive new services from outside their homes.

[05] In general, a home network system refers to a network that incorporates home information devices including personal computers into one system to enable communications therebetween. The home network system has rapidly spread together with developments in networking technologies, support software, and information appliances.

[06] Wirings built into homes, such as existing phone lines (Home PNA: Home Phoneline Networking Alliance), electric power outlets (power line LAN), coaxial cables for TV, and so on, are utilized to build such a home network system, and FIG. 1 is a view for conceptually showing such a home network system.

[07] First and second home gateways 110 and 210 are provided in first and second home networks 100 and 200, respectively. Home devices 111, 113, 115, and 117, and home devices 211 and 213 are respectively interconnected to the first and second home gateways 110 and 210 for networking, and connected to external networks through the first and second home gateways 110 and 210.

[08] If a new device is connected to a home network in such a conventional home network, there is no authentication process for the device in general. That is, in the event that a new device 113 is connected to the first home network 100, the new device 113 is physically connected to the first home gateway 110 and transfers connection information, so that the new device 113 is connected to the first home gateway 110. Thus, the conventional home network has a unilateral structure in that only the first home gateway 110

authenticates the new device 113. Therefore, the connection information of the new device 113 is transferred to the second home gateway 210 of the second home network 200 adjacent to the first home network 100, through the wirings such as phone lines, electric power line LAN, TV coaxial cables, and so on. Accordingly, either by accident or on purpose, the home device 113 of the first home network 100 is connected to the second home network, by which the first home network 100 is exposed to the second home network 200.

[09] As described above, the conventional home network has a problem with respect to privacy and security since it has no authentication process for home devices connected thereto.

SUMMARY

[10] The present invention has been devised to solve the above problem, so it is an aspect of the present invention to provide a home device authentication system and a method performing a home device authentication process for home network privacy and security.

[11] In order to achieve the above aspect, a home device authentication system comprises one or more home devices each having device information including coding information for authentication and information on a service provider providing authentication services; and a home gateway including decoding information corresponding to the coding information of the home devices, and for authenticating the home devices by using the decoding information.

[12] The home device authentication system further comprises a service provider providing the decoding information, wherein, if there exists no decoding information in the home gateway, the home gateway requests the decoding information to the service provider.

[13] The home gateway includes an input/output unit for inputting the device information including the coding information and the service provider information; a device process unit for obtaining the decoding information, authenticating the home device by using the decoding information and the coding information, and selecting a display device for displaying a performed authentication result; and an application process unit for generating an authentication request screen requesting to a user whether to approve the authentication result.

[14] The input/output unit outputs the authentication request screen to the selected display device, and the device process unit controls the input/output unit to set or not to set the home devices to the home network based on whether or not the user approves the result through the authentication request screen.

[15] The home gateway further includes a display unit for externally displaying the authentication result; and a user input unit for inputting a selection command with respect to whether a user approves the result in correspondence to the displayed authentication result.

[16] The device process unit controls the input/output unit to set or not to set the home devices to the home network in correspondence to the user's selection command inputted from the user input unit.

[17] The device process unit controls the input/output unit to cut off setting the home devices to the home network if a response signal with respect to a user's approval is not inputted for a predetermined period of time.

[18] The device process unit includes a information detection unit for detecting the coding information and the service provider information inputted from the input/output unit; an authentication process unit for authenticating the home devices by using the decoding information and the coding information, and controlling setting of the home devices to the home network according to whether there is a user's approval in the authentication request screen; a storage for storing information on the home devices connected to the home network and the decoding information corresponding to the coding information for the home devices; and a selection unit for selecting a displayable device for the authentication result performed in the authentication process unit based on information on the home devices that is previously stored.

[19] The authentication process unit stores the home device information into the storage, if the setting of the home devices to the home network is approved according to the user's approval.

[20] In the meantime, a home device authentication method according to the present invention comprising steps of inputting device information

including coding information for authenticating home devices and information on a service provider providing authentication services; authenticating the home devices by using previously stored decoding information corresponding to the coding information, and selecting a device capable of displaying an authentication result; and generating an authentication request screen requesting a user's approval with respect to the authentication result.

[21] The home device authentication method further comprises a step of requesting the decoding information to a service provider by using the service provider information, if there exists no decoding information in the home device process step.

[22] The home device authentication method further comprises steps of outputting the generated authentication request screen to the display device; and setting or cutting off the home devices to or from the home network depending upon whether or not the user approves the authentication result through the authentication request screen.

[23] The home device authentication method further comprises steps of externally displaying the authentication result; and inputting a selection command with respect to whether a user approves the result in correspondence to the displayed authentication result.

[24] The step for setting or cutting off the home devices sets or cuts off the home devices to or from the home network in correspondence to the user's selection command inputted from the user input step, and cuts off setting the

home devices to the home network if a response signal with respect to a user's approval is not inputted for a predetermined period of time.

[25] The device process step includes steps of detecting the device information including the coding information and the service provider information that are inputted; authenticating the home devices by using the decoding information and the coding information, and controlling setting or cutting-off of the home devices to or from the home network according to whether there is a user's approval in the authentication request screen; and selecting a displayable device for the authentication result performed in the authentication process step based on information on the home devices connected to the home network.

[26] Preferably, but not necessarily, the home device authentication method further comprises a step of storing the information on the home devices if the setting of the home devices to the home network is approved according to the user's approval.

[27] Accordingly, the process for authenticating devices connected to a home network can prevent the devices from being connected by accident or on purpose to different networks. By doing so, the privacy and security for a network system can be secured. Further, even users unfamiliar with home network environments can install and register home devices in a more convenient manner.

BRIEF DESCRIPTION OF THE DRAWINGS

[28] The invention will be described in detail with reference to the following drawings in which like reference numerals refer to like elements, and wherein:

[29] FIG. 1 is a conceptual view for showing a conventional general home network system;

[30] FIG. 2 is a schematic view for showing a structure of a home device authentication system according to an exemplary embodiment of the present invention;

[31] FIG. 3 is an exemplary view for showing device information(DI) included in a device 311 according to an exemplary embodiment of the present invention;

[32] FIG. 4 is a detailed block diagram for showing a home gateway 330 according to an exemplary embodiment of the present invention;

[33] FIG. 5 is a detailed block diagram for showing a device processor 333 for a home gateway 330 according to an exemplary embodiment of the present invention;

[34] FIG. 6 is an exemplary view for showing an authentication request screen 600 for a new device according to an exemplary embodiment of the present invention; and

[35] FIG. 7 is a view for showing a flow chart for a home device authentication process according to an exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE EXEMPLARY EMBODIMENTS

[36] Hereinafter, the present invention will be described in detail with reference to the accompanying drawings.

[37] FIG. 2 is a conceptual view for explaining a home device authentication system according to an exemplary embodiment of the present invention.

[38] A home device authentication system has a home device 311 newly connected to a home network 300, a home gateway 330 performing a server function for the home network 300, and a service provider 400 providing predetermined coding information for authenticating the new device 311.

[39] First, the home device 311 according to the present invention has device information (DI) as shown in FIG. 3. The device information (DI) includes at least general device specification information (I1), service provider information (I2) for providing device authentication services, and predetermined coding information(I3) for performing a device authentication process.

[40] The home gateway 330, as shown in FIG. 4, has an input/output unit 331 connected with a home device of a home network through various wired and/or wireless manners and for inputting and outputting data based on a network protocol such as the Dynamic Host configuration Protocol (DHCP), a device process unit 333 for authenticating the new device 311, an application process unit 335 for applying an application program for providing device authentication services, a display unit 337, such as LED, for notifying users of

information corresponding to authentication results, a user input unit 339, such as an operation panel, for inputting user's operation commands, and so on.

[41] The service provider 400 provides to the home gateway 330 predetermined coding information corresponding to the new device 311 requested from the home gateway 330 in order to authenticate the new device 311 connected to the home gateway 330.

[42] FIG. 5 is a detailed block diagram for showing the device process unit 333 of the home gateway 330 according to an exemplary embodiment of the present invention, and the operations of the device process unit 333 are described in detail with reference to FIG. 4 and FIG. 5.

[43] The device process unit 333 includes at least, an information detection unit 333-1, a storage 333-4, an authentication process unit 333-2, and a selection unit 333-3.

[44] The information detection unit 333-1, if the new device 311 is physically connected to a home network, recognizes a newly connected device based on information of the new device 311 that is inputted from the input/output unit 331, and detects the inputted device information D1 as shown in FIG. 3.

[45] The storage 333-4 stores information and the like with respect to home devices connected to the home gateway 330, and, further, has decoding information corresponding to the coding information on individual home devices. In general, the kind of decoding information is provided by the home device manufacturer.

[46] The authentication process unit 333-2 authenticates the new device 311 by using a predetermined authentication algorithm. That is, the authentication process unit 333-2 performs an authentication process for the new device 311 by using information provided for authentication from the device information D1 of the new device 311. For example, the information includes the service provider information I2 and the coding information I3 from the device information D1 shown in FIG. 3.

[47] Descriptions will be made on an authentication process by using the public key algorithm and the hash algorithm, for example, as authentication algorithms.

[48] First, the authentication process unit 333-2 checks for a public key of the decoding information previously stored in the storage 333-4 based on the manufacturer's general device specification information I1 from the device information DI of the new device 311. That is, the authentication process unit 333-2 checks whether there exists a public key of the decoding information corresponding to a signature of coding information I3 of the new device 311.

[49] If there exists a public key corresponding to the signature of the new device 311 in the storage 333-4, the authentication process unit 333-2 decodes the signature by using the public key.

[50] Here, the signature is an obtained hash value that is coded using a private key, wherein a predetermined message is shortened into a hash and a hash value is obtained from the hash. That is, the authentication process unit 333-2 decodes the signature of private key using a public key, to thereby

recover an original hash value. Accordingly, the authentication process unit 333-2 obtains a hash value for a message, compares the obtained hash value with a recovered original hash value, and decides whether the message is normal or not.

[51] In the meantime, if there exists no decoding information corresponding to a signature of coding information I3 on the new device 311 as a result of the check on the decoding information previously stored in the storage 333-4, the authentication process unit 333-2 requests a public key of the device to a service provider, using the service provider information I2 from the inputted device information DI. The authentication process unit 333-2, if the public key is provided from the service provider, decodes the signature of the coding information I3 using the public key.

[52] The selection unit 333-3 searches for information on individual home network devices that is stored in the storage 333-4 and selects an optimum display device that can display an authentication request screen to be described later. Preferably, but not necessarily, the selection unit 333-3 selects a displayable device that is used most recently.

[53] As stated above, to the application process unit 335 of the home gateway 330 is provided the authentication result processed in the authentication process unit 333-2 and information on the displayable device selected from the selection unit 333-3. The application process unit 335 generates an authentication request screen 600, as shown in FIG. 6, having a portion A1 for displaying the authentication result to a user and a portion A2

for requesting device authentication. The authentication request screen 600 generated as above is transferred to a selected display device, and a user decides whether to authenticate the new device 311 through the authentication request screen 600 displayed.

[54] If a current home network does not have a device capable of displaying the authentication request screen 600, it is decided whether to authenticate the new device through the display unit 337, such as, for example, LED, and the user input unit 339 of the home gateway 330.

[55] For example, the display unit 337 notifies a user of the authentication result by turning on a blue LED if the authentication process unit 333-2 authenticates as an authorized device the device 311 newly connected to the home gateway 330, and, to the contrary, by turning on a red LED if the new device 331 is an alien device that is unauthorized as a result of the authentication result therefor. Accordingly, the user decides whether to authenticate the new device through the user input unit 339.

[56] As above, it is decided whether or not the new device 311 is set to a home network based on whether a user authenticates the new device 311 or not, so privacy or security is secured for the home network, and, further, servicing users for home device installation and registration can promote convenience in use. When the device is set to the network, the device remains connected to the network.

[57] Hereinafter, detailed descriptions are made on an authentication process for a home device newly connected to a home network with reference to FIG. 7 showing a flow chart for a home device authentication process.

[58] First, the new device 311 is physically connected to the home gateway 330, and, at this time, the device information DI provided from a new device manufacturer is transferred to the input/output unit 331 in a DHCP broadcast message format.

[59] The information detection unit 333-1 recognizes a connection of the new device 311 based on the device information DI of the new device 311 that is inputted to the input/output unit 331 of the home gateway 330, and detects the device information (device information DI illustrated in FIG. 3).

[60] The device information DI detected from the information detection unit 333-1 is transferred to the authentication process unit 333-2.

[61] The authentication process unit 333-2 authenticates the new device using the device information DI.

[62] First, it is checked whether there exists a public key of the decoding information corresponding to a signature of coding information I3 of the new device 311 from the decoding information previously stored in the storage 333-4. If there exists in the storage 333-4, the public key corresponding to the signature of the new device 311 as a result of the check, the signature is decoded by using the public key.

[63] In the meantime, if the decoding information does not exist, the service provider information I2 is used to request the public key from a service

provider. The authentication process unit 333-2 uses the provided public key to decode the signature of coding information I3, and decides whether it is authorized device information.

[64] Further, if a device is not registered or device information is different from information provided from the service provider at the beginning in a process for obtaining a public key from the storage 333-4 and the service provider, it is decided that the device is not an authorized device, so it can be cut off from a network.

[65] The selection unit 333-3 selects an optimum display device, for example, a display device used most recently that can display the authentication request screen 600 based on home network device information stored in the storage 333-4.

[66] To the application process unit 335 is transferred the authentication result processed in the authentication process unit 333-2 and display device information selected in the selection unit 333-3, and the application process unit 335 generates the authentication request screen 600 as shown in FIG. 6. The authentication request display 600 is displayed on a selected display device, and it is decided by a user whether to authenticate the new device.

[67] The user decides the authentication for a device based on device information including the authentication result displayed on the authentication request screen 600. For example, if it is decided as the authentication result that the new device 311 is an authorized and normal device, a user selects 'YES' to authenticate the new device 311 to be set to a network. The

authentication signal 'YES' is transferred to the application process unit 335 of the home gateway 330, and the application process unit 335 transfers to the authentication process unit 333-2 a registration signal for the new device 311 corresponding to the authentication signal 'YES'. Accordingly, the authentication process unit 333-2 stores the device information of the new device 311 into the storage 333-4, and controls the input/output unit 331 to proceed with network setting for the new device 311.

[68] In the meantime, if it is decided as the authentication result for the new device 311 that the new device 311 is an unauthorized and abnormal device, the user selects 'NO' to prevent the new device 311 from being set to a network. Further, if there is no response signal from a user with respect to the authentication for a predetermined period of time, the network setting for the new device 311 is automatically cut off.

[69] If a rejection signal 'NO' is inputted to reject the authentication or there is no response signal from a user for a predetermined period of time, the application process unit 335 transfers to the authentication process unit 333-2 an authentication rejection signal with respect to the new device 311. The authentication process unit 333-2 controls the input/output unit 331 not to set the new device 311 to a network.

[70] In the home device authentication system as above, a new device undergoes an authentication process by means of a predetermined coding algorithm during the registration to a home network, and then it is decided whether the new device is registered to a network based on whether a user

authenticates the device. Accordingly, privacy and security for a home network can be secured.

[71] First, the present invention performs an authentication process for a device connected to a home network, so it can prevent a device of a different network from being connected to the home network by accident or on purpose. By doing so, the privacy and security for a network system can be secured.

[72] Second, a user unfamiliar with home network environments can install and/or register a home device in a more convenient manner.

[73] While the invention has been shown and described with reference to certain exemplary embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the spirit and scope of the invention as defined by the appended claims.